Managing Supply Chain Risk

Using NIST Standards and Guidelines

ICT Supply Chain Risk Management Workshop

October 15, 2012

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

The Current Landscape.

It’s a dangerous world when it comes to cyber…

Conventional Threats

- *What do we worry about?*
  - Hostile cyber attacks
  - Natural disasters
  - Structural failures
  - Human errors of omission or commission

Advanced Persistent Threat

An adversary that —

- Possesses significant levels of expertise / resources.
- Creates opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, deception).
- Establishes footholds within IT infrastructure of targeted organizations:
  - To exfiltrate information.
  - Undermine / impede critical aspects of a mission, program, or organization.
  - Position itself to carry out these objectives in the future.

Unconventional Threats

What should we worry about?

Complexity

Connectivity

Culture

The federal cyber security strategy…

Build It Right, Then Continuously Monitor

The First Front.

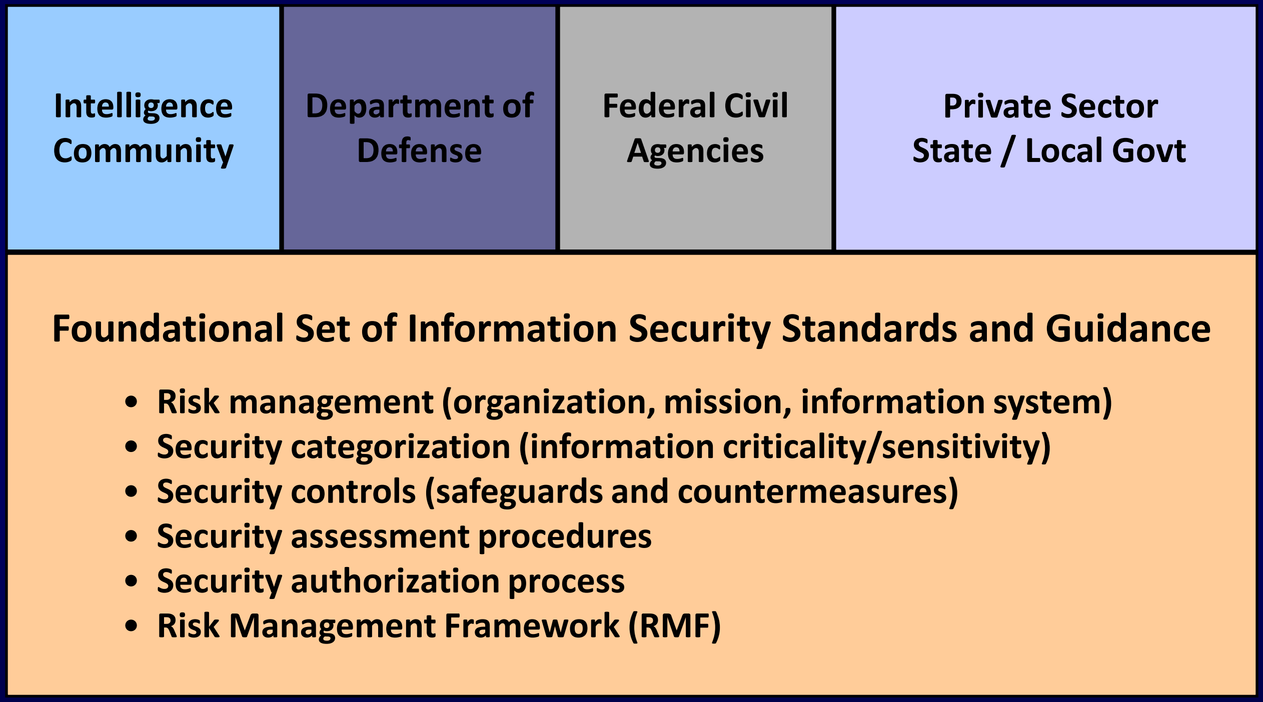
What we have accomplished…

Joint Task Force Transformation Initiative

- In 2012, completed development of comprehensive security guidelines that can be adopted by all federal agencies including the national security community.
- Flexible and extensible tool box includes:
  - *An enterprise-wide risk management process.*
  - *State-of-the-practice, comprehensive, security controls.*
  - *Risk management framework.*
  - *Risk assessment process.*
  - *Security control assessment procedures.*

Unified Information Security Framework

Generalized Model



***Unique* Information Security Requirements**

The "Delta"

Intelligence Community

Department of Defense

Federal Civil Agencies

Private Sector State / Local Govt

***Common* Information Security Requirements**

Foundational Set of Information Security Standards and Guidance

- Risk management (organization, mission, information system)
- Security categorization (information criticality/sensitivity)
- Security controls (safeguards and countermeasures)
- Security assessment procedures
- Security authorization process
- Risk Management Framework (RMF)

National security and non national security information systems

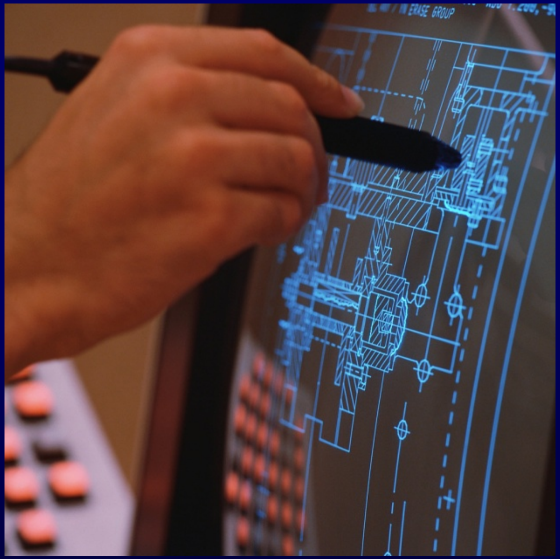
Key Publications in the Framework

- NIST Special Publication 800-39
  Managing Information Security Risk:
  Organization, Mission, and Information System View
- NIST Special Publication 800-30
  Guide for Conducting Risk Assessments
- NIST Special Publication 800-37
  Applying the Risk Management Framework
  to Federal Information Systems
- NIST Special Publication 800-53
  Recommended Security Controls for Federal
  Information Systems and Organizations
- NIST Special Publication 800-53A
  Guide for Assessing the Security Controls
  in Federal Information Systems and Organizations

The Second Front.

What we need to accomplish…

We need to build our security programs like NASA builds space shuttles— using the *integrated project team* concept.



A New Approach for Information Security

- Work directly with mission/business owners and program managers.
- Bring all stakeholders to the table with a vested interest in the success or outcome of the mission or business function.
- Consider information security requirements as mainstream functional requirements.
- Conduct security trade-off analyses with regard to cost, schedule, and performance requirements.
- Implement enforceable metrics for key officials.

What can we do to change course?

Simplify, Specialize, and Integrate…

Increasing Strength of IT Infrastructure

- Simplify.
  - Reduce and manage *complexity* of IT infrastructure.
  - Use enterprise architecture to streamline the IT infrastructure; *standardize*, *optimize*, *consolidate* IT assets.
- Specialize.
  - Use guidance in SP 800-53, Rev 4 to *customize security plans* to support specific missions/business functions, environments of operation, and technologies.
  - Develop effective *monitoring strategies* linked to specialized security plans.

Increasing Strength of IT Infrastructure

- Integrate.
  - Build information security requirements and controls into mainstream organizational processes including:
    - *Enterprise Architecture*.
    - *Systems Engineering*.
    - *System Development Life Cycle*.
    - *Acquisition*.
  - Eliminate information security programs and practices as stovepipes within organizations.
  - Ensure information security decisions are risk-based and part of routine *cost*, *schedule*, and *performance* tradeoffs.

Complexity.

Ground zero for our current problems…

Information security and privacy, traditional societal values, are at greater risk today due to the ever increasing size of our *digital footprint*…

If we can’t understand it –

we can’t protect it…

Enterprise Architecture

- Consolidation.
- Optimization.
- Standardization.

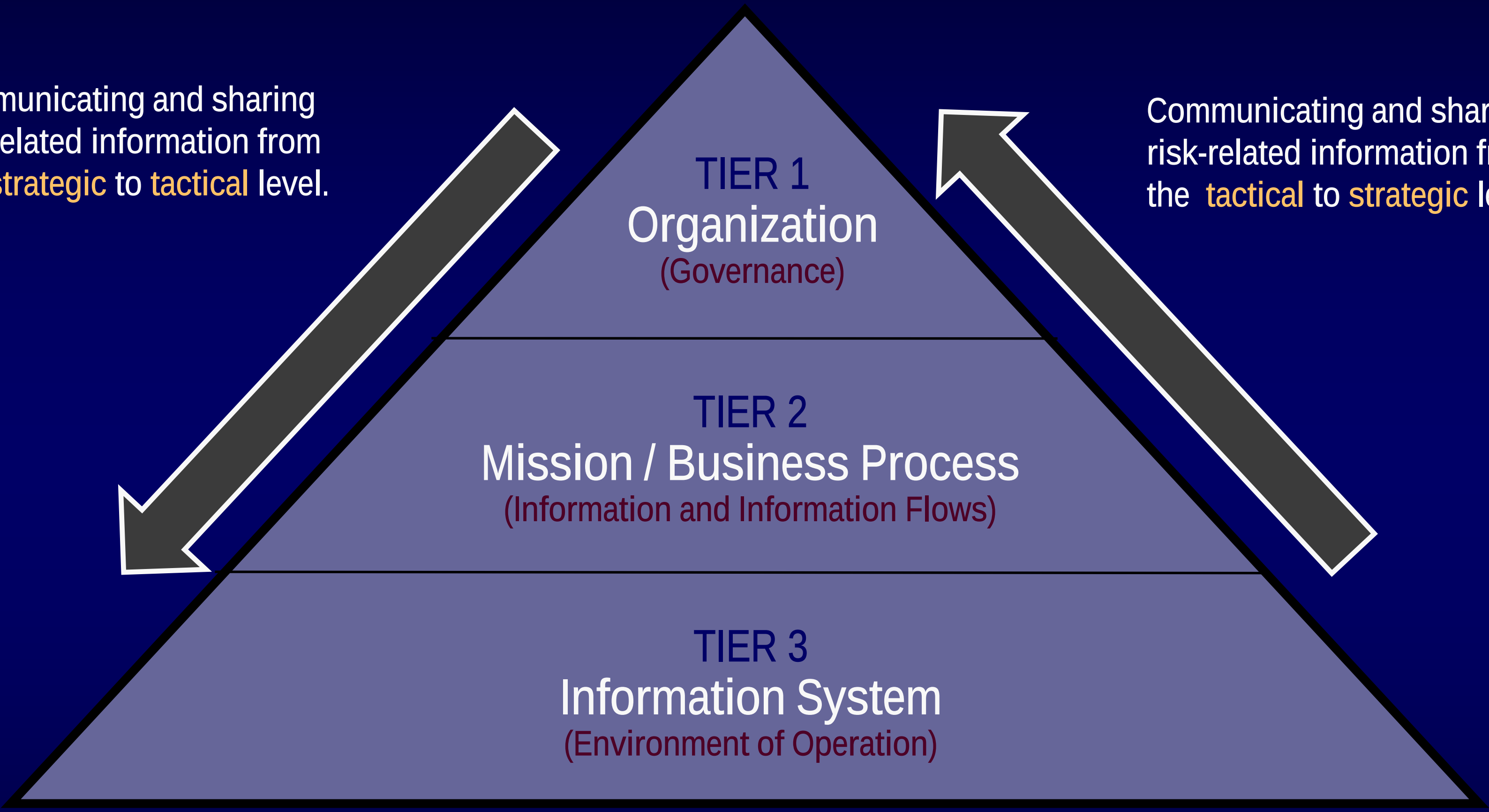
And the integration of information security requirements…

- Reduces the size and complexity of IT infrastructures, promotes good information security and privacy, and can potentially lower costs (significantly) for organizations.

Think strategic.

Execute tactical…

STRATEGIC RISK FOCUS



Communicating and sharing risk-related information from the strategic to tactical level.

TIER 1
Organization
(Governance)

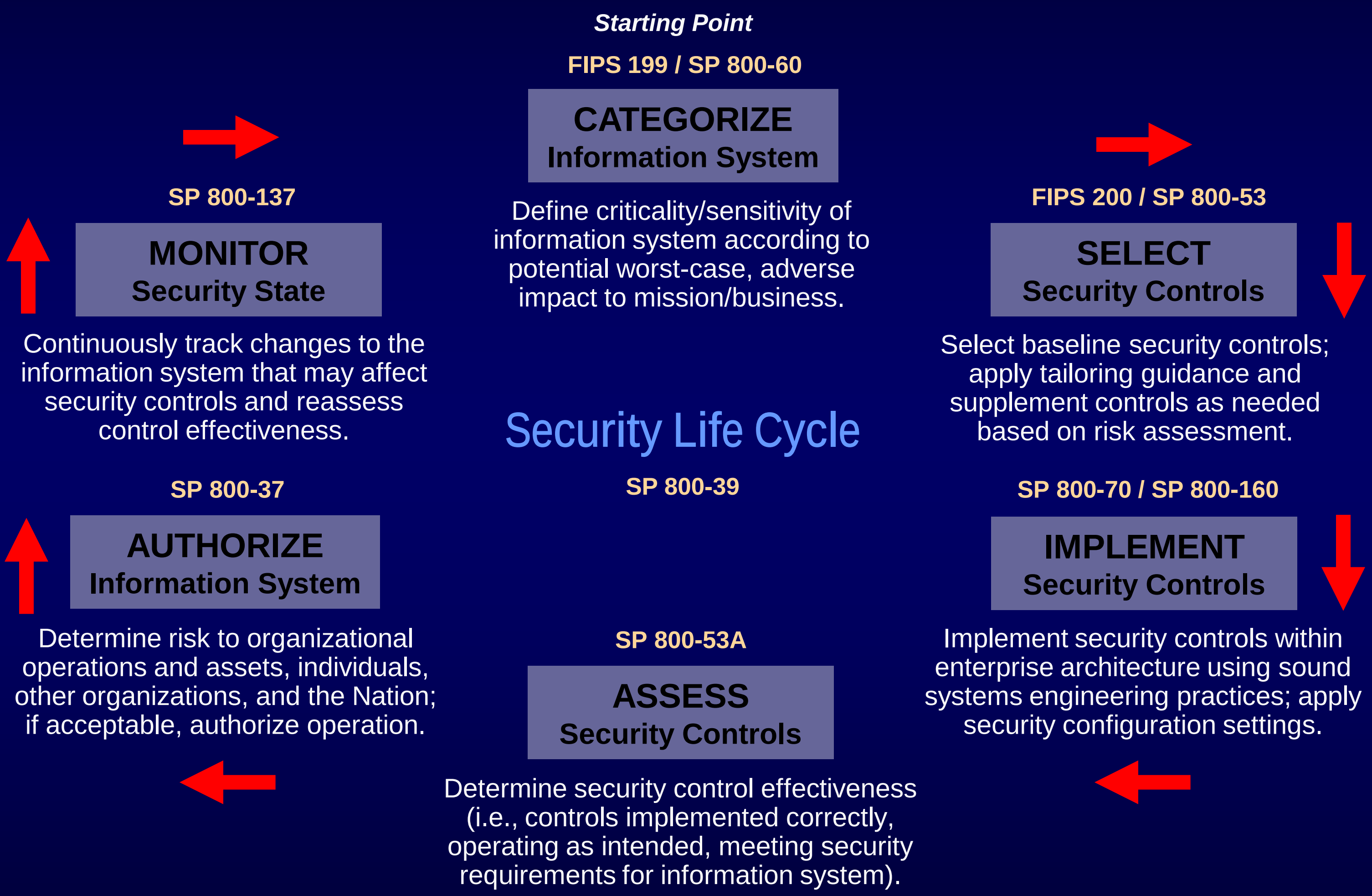
TIER 2
Mission / Business Process
(Information and Information Flows)

TIER 3
Information System
(Environment of Operation)

Communicating and sharing risk-related information from the tactical to strategic level.

TACTICAL RISK FOCUS

Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200 / SP 800-53

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70 / SP 800-160

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-37

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-137

MONITOR
Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

SP 800-39

Defense-in-Depth

Links in the Security and Privacy Chain: Security and Privacy Controls

- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical and personnel security
- ✓ Security assessments and authorization
- ✓ Continuous monitoring
- ✓ Privacy protection

- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms
  (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices
  (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

Adversaries attack the weakest link…where is yours?

Defense In Depth is a Good Strategy

Until it fails…then what?

Resilience.

The only way to go for critical missions and information systems…

Functionality and Assurance.

They ride together…

FUNCTIONALITY

What is observable in front of the wall.

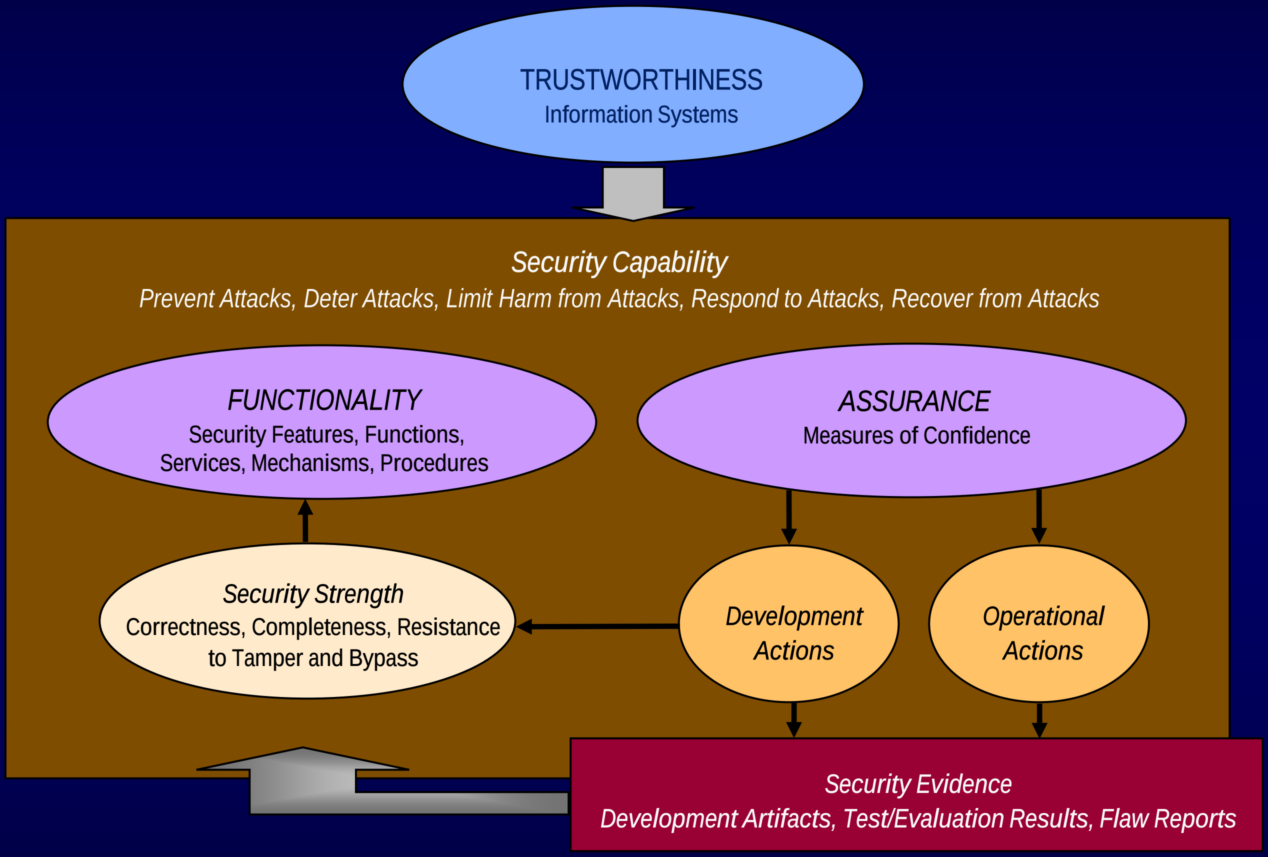
What is observable behind the wall.

ASSURANCE

Assurance.

You don’t need it until you need it…

Assurance and Trustworthiness



TRUSTWORTHINESS
Information Systems

Security Capability
Prevent Attacks, Deter Attacks, Limit Harm from Attacks, Respond to Attacks, Recover from Attacks

FUNCTIONALITY
Security Features, Functions, Services, Mechanisms, Procedures

ASSURANCE
Measures of Confidence

Security Strength
Correctness, Completeness, Resistance to Tamper and Bypass

Development Actions

Operational Actions

Security Evidence
Development Artifacts, Test/Evaluation Results, Flaw Reports

Enables Understanding of Security Capability

And after we build it right.

What next?

Continuous Monitoring

- Determine effectiveness of risk responses.
- Identify changes to information systems and environments of operation.
- Verify compliance to federal legislation, Executive Orders, directives, policies, standards, and guidelines.

Bottom Line: Increase situational awareness to help determine risk to organizational operations and assets, individuals, other organizations, and the Nation.

And until we build it right.

What should we do?

Important Stop-Gap Actions

- For high-end adversaries launching sophisticated and well-coordinated cyber attacks targeting: U.S. critical infrastructure; federal mission-essential functions and systems; and private sector industries—
  - ✓ Develop, implement, and exercise robust contingency plans to support full scale continuity of operations;
  - ✓ Implement continuous monitoring programs; and

Special Publication 800-53, Revision 4.

Big changes on the way…

Major Drivers for Update

- Current threat landscape.
- Empirical data obtained from cyber attacks.
- Gaps in coverage in current security control catalog.
- Insufficient attention to security assurance and trustworthiness.
- Need for additional tailoring guidance for specific missions, technologies, and environments of operation.

Gap Areas Addressed

- Insider threat
- Application security
- *Supply chain risk* ICT
- Security assurance and trustworthy systems
- Mobile and cloud computing technologies
- Advanced persistent threat
- Tailoring guidance and overlays
- Privacy

SP 800-53 Supply Chain Control

- FAMILY: SYSTEM AND SERVICES ACQUISITION

  SA-12 Supply Chain Protection

  Control: The organization protects against supply chain threats by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy.

Supply Chain Control Enhancements

- SA-12 SUPPLY CHAIN PROTECTION
  - *ACQUISITION STRATEGIES / TOOLS / METHODS*
  - *SUPPLIER REVIEWS*
  - *LIMITATION OF HARM*
  - *ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE*
  - *USE OF ALL-SOURCE INTELLIGENCE*
  - *UNAUTHORIZED MODIFICATIONS*

Supply Chain Control Enhancements

- SA-12 SUPPLY CHAIN PROTECTION
  - *VALIDATE AS GENUINE AND NOT ALTERED*
  - *PENETRATION TESTING / ANALYSIS OF SUPPLY CHAIN ELEMENTS*
  - *INTER-ORGANIZATIONAL AGREEMENTS*
  - *CRITICAL INFORMATION SYSTEM COMPONENTS*
  - *PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES*

Potential Supply Chain Changes

Under Consideration for SP 800-53. Revision 4

- Additional enhancements and supplemental guidance for SA-12 and supply chain-related controls—
  - Identification of critical functions and components.
  - Identity and traceability of supply chain elements.

Adversaries are not ten feet tall.

They have work factors and attack sequences that can be disrupted…

Managing supply chain risk.

Doesn't mean fixing everything…

- ✓ Frame
- ✓ Assess
- ✓ Respond
- ✓ Monitor

Risk Tolerance.

How you know when to stop deploying security controls…

On The Horizon

- NIST Special Publication 800-53, Revision 4.
  Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-53A, Revision 2.
  Guide for Assessing the Security Controls in Federal Information Systems and Organizations
- NIST Special Publication 800-160. New
  Security Engineering Guideline
- NIST Special Publication 800-161 New
  Supply Chain Practices for Federal Information Systems

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov